Dagboek van



een computer



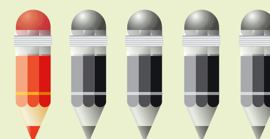
Niet alleen staatsinstanties registreren nauwgezet je handel en wandel. Ook je besturingssysteem en allerlei services en toepassingen houden vaak bij wat je allemaal uitvoert. Ze gebruiken daarvoor gedetailleerde logboeken, die vooral bij problemen hun nut bewijzen. CEDRIC MESKENS

Je zou ervan versteld staan wat je pc allemaal bijhoudt tijdens een doordeweekse computersessie. Neem nu een onschuldig bezoek aan een website. Om te beginnen houdt je browser standaard alle bezochte sites bij in zijn geschiedenis, belanden er heel wat gegevens bij de tijdelijke internetbestanden en worden er wellicht ook cookies op je schijf geplant. Het is evenmin uitgesloten dat je onderweg op een site botst die heimelijk een stukje malware in je systeem wil planten, wat je antivirusprogramma en firewall de nodige stof geeft voor hun eigen logs. En ben je wel zeker dat je ouders of partner stiekem geen keylogger hebben geïnstalleerd, die letterlijk elke toetsaanslag registreert? Behoorlijk paranoïde toestanden dus, en het hoeft dan ook niet te verbazen dat je via specifieke software – zoals het gratis CCleaner **www.ccleaner.com** – allerlei logbestanden kan verwijderen.

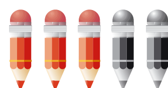
In dit artikel pakken we het anders aan: in plaats van logboeken te verwijderen, willen we een aantal ervan nader bekijken. Ze kunnen namelijk ook erg leerzaam zijn. Waarom heeft Windows of een of andere toepassing er plots de brui aan gegeven, welke snoodaard probeerde je systeem te hacken, hoeveel gigabytes heeft zoonlief alweer opgesoupeerd en welke foute sites heeft hij dit keer weer 'per ongeluk' bezocht? Het antwoord vind je misschien wel in de logboeken.

Van eenvoudig naar aartsmoeilijk...

Niet alle logbestanden zijn even doorgrondelijk. Om je toch een indicatie te geven van de moeilijkheidsgraad, werken we met potloden. 1 potlood betekent dat iedereen het logboek zou moeten kunnen begrijpen, terwijl je bij vijf potloden al een gevorderde computergebruiker moet zijn.



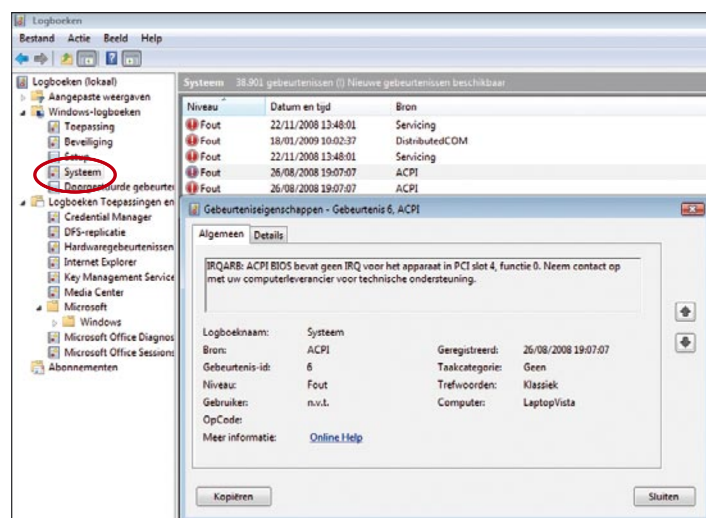
Windows logboeken



Iedereen heeft het wel eens meegemaakt: Windows zwaait je plots uit met een bluescreen of een toepassing crasht telkens je die opstart. Begin dan de zoektocht naar de oorzaak in de logboeken van Windows. Het besturingssysteem houdt namelijk in alle stilte een reeks logboeken bij van belangrijke systeemgebeurtenissen, inclusief de fouten. Open daarvoor het Windows **Configuratiescherm** in **Klassieke weergave** en klik achtereenvolgens op **Systeembeheer** en op **Logboeken** – of tik *eventvwr.msc* in bij **Uitvoeren** (XP) of **Zoekopdracht starten** (Vista).
In het volgende dialoogvenster krijg je links een overzicht van de verschillende logboeken en rechts de inhoud van het geopende exemplaar. Loopt er iets spaak in Windows, dan kijk je best in het logboek **Systeem**, terwijl je bij een manke toepassing beter aanklopt bij **Toepassing**. Vista gooit er nog een paar logboeken bovenop: **Setup**, met gegevens over de installatie van nieuwe programma's, en een aantal bij elkaar geharkte exemplaren in de rubriek **Logboeken Toepassingen en Services**. Daar vind je onder meer logboeken van Vista-tools als Backup, Readyboost en ParentalControls (ouderlijk toezicht).

OP ZOEK NAAR DE FOUT

Zoals je merkt, worden de gebeurtenissen in zo'n logboek standaard chronologisch opgelijst. Concentreer je vooral op de gebeurtenissen van het type **Fout** en in mindere mate op die van het type **Waarschuwing**. Met een dubbelklik op het bewuste item roep je een venster op met gedetailleerde informatie over de gebeurtenis. Je treft hier ook een link aan die je mogelijk naar enkele handige raadgevingen voert. Word je hier niet wijzer van, dan kan je altijd nog je licht opsteken door een deel van de foutbeschrijving als zoekterm in Google in te tikken – probeer je geluk zeker ook bij Google's



Windows – en vooral Vista – houdt in alle stilte een aantal logboeken bij.



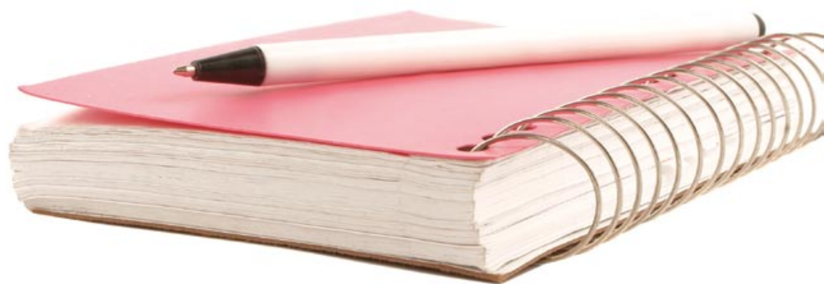
tip

Start Windows niet meer op de normale manier op, probeer de logboeken dan ***vanuit veilige modus*** *op te starten: hou even de F8-toets ingedrukt net voor Windows opstart.*

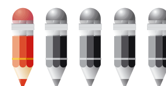
Discussiegroepen. Op deze manier hebben we zelf al vaker problemen weten te verhelpen. Of je noteert de informatie die je bij **Bron** en **Gebeurtenis-id** aantreft, waarna je een bezoekje brengt aan www.microsoft.com/technet/support/eventserrors.mspx. Bij **Microsoft Product** selecteer je **Windows Operating System** en vervolgens vul je de genoteerde gegevens in bij **Gebeurtenisbron** en **Id**. De taal kan je op **Dutch** geselecteerd laten, maar de Engelstalige databank blijkt wel een stuk uitgebreider. Tot slot hoef je alleen nog op de knop **Zoeken** te drukken en hopen dat je waardevolle feedback krijgt.

Logboeken via e-mail

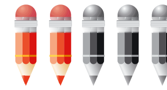
De aard van het beestje vereist natuurlijk dat je bij mogelijke problemen telkens zelf de logboeken moet induiken. Best vervelend, maar dat is buiten EventSentry www.eventsentry.com gerekend – waarvan je (na registratie) trouwens ook een gratis Light-editie kan downloaden. We kunnen hier niet alle mogelijkheden van deze tool bespreken, maar als je na installatie de rubriek **Packages, Event Log Packages, Default, Warnings & Errors** opent, beland je in een dialoogvenster, waar je zelf tot in de kleinste details kan instellen bij welk soort gebeurtenissen je bijvoorbeeld automatisch een e-mailtje wil ontvangen.



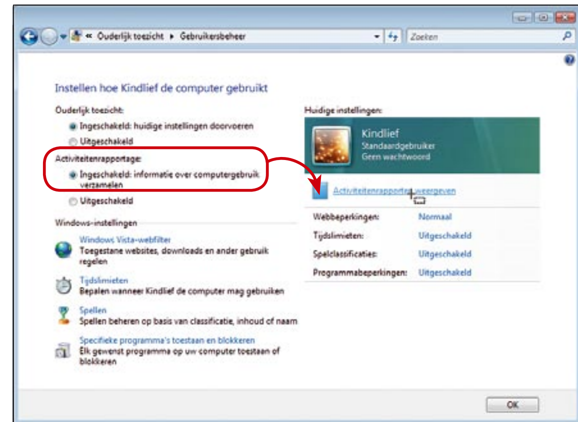
Windows Live Messenger



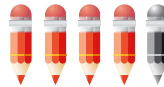
Heel wat lichtvoetiger van aard zijn de logboeken van Windows Live Messenger: hierin vind je gewoon alle MSN-gesprekken terug. Dat kan interessant zijn als je bijvoorbeeld nog eens wil nalezen welke beloftes je gesprekspartner allemaal gedaan heeft. Open het menu van Windows Live Messenger en kies achtereenvolgens **Extra, Opties**. Ga vervolgens naar de rubriek **Berichten**; onderaan lees je waar de bestanden bewaard worden. Blader vervolgens naar deze map. Daar tref je voor elke gesprekspartner een ander xml-bestand aan. Een dubbelklik volstaat om zo'n bestand in leesbare vorm te openen. De gevoerde dialogen krijg je netjes gepresenteerd in chronologische volgorde. Wil je deze berichtgeschiedenis niet langer laten bijhouden, verwijder dan het vinkje bij **Gesprekken automatisch in een bestand opslaan** in het **Opties**-venster van Windows Live Messenger.

Ouderlijk toezicht (Vista) 

In Windows Vista zit een krachtige module voor ouderlijk toezicht. Natuurlijk hoort hier ook een uitgebreide rapportering bij. Open dus het Windows **Configuratiescherm** in **Categorieweergave** en klik op **Ouderlijk toezicht voor elke gebruiker instellen**, waarna je een van de (standaard)accounts van je kinderen selecteert. In het volgende venster stip je de optie **Ingeschakeld: huidige instellingen doorvoeren** aan. Wil je logs van het internetgebruik van je kind bijhouden, vink dan zeker ook **Ingeschakeld: informatie over computergebruik verzamelen** aan. Vervolgens kan je het Ouderlijk toezicht finetunen door de links **Windows Vista-webfilter**, **Tijdslimieten**, **Spellen** en **Specifieke programma's toestaan en blokkeren** aan te klikken. Ons interesseert echter vooral de rapporteringsfunctie, en die is heel erg uitgebreid. Meld je aan met je eigen account, open opnieuw de module voor Ouderlijk toezicht en klik op **Activiteitenrapport weergeven.** Je krijgt voor elk gemonitord kind een indrukwekkend aantal (sub)rubrieken te zien, waaronder de top 10 van de bezochte websites, de 10 meest recent geblokkeerde sites, welke games hij heeft gespeeld, welke bestanden hij heeft proberen te downloaden, enzovoort. Hou er wel rekening mee dat Vista zo'n rapport alleen van de laatste 7 dagen bijhoudt. Wel is het op elk moment mogelijk het rapport op te slaan in html-formaat en bij te houden via de link **Rapport maken.**



Volg de digitale exploten van je kind op de voet...

Windows Firewall 

De firewall in Windows XP en Vista is in de eerste plaats bedoeld om indringers buiten te houden, hoewel in Vista ook ongewenst verkeer in omgekeerde richting (van binnen naar buiten) kan worden geblokkeerd. Standaard houdt deze firewall geen logboek bij, maar je kan dat wel instellen. In Windows XP open je hiervoor het **Configuratiescherm** en selecteer je **Windows Firewall.** Ga naar het tabblad **Geavanceerd** en druk op de tweede knop **Instellingen.** Via de knop **Opslaan als** leg je de locatie van het logboek vast en met vinkjes geef je te kennen of je alleen de verloren pakketten wil registreren of ook de geslaagde verbindingen in het logboek. In Vista ga je enigszins anders te werk. Tik de opdracht *firewall* in bij **Zoekopdracht starten** en klik in het startmenu op de optie **Windows Firewall met geavanceerde beveiliging.** In het middenpaneel klik je vervolgens op de link **Eigenschappen van Windows Firewall.** Open nu het gewenste firewallprofiel (bijvoorbeeld: **Openbaar profiel**) en druk op de onderste knop **Aanpassen:** je krijgt nu ongeveer dezelfde opties te zien als bij XP.

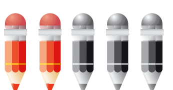
Het logbestand zelf kan je eenvoudigweg openen met je Kladblok (of in Excel) – desnoods kopieer je het eerst naar een andere locatie. Je kijkt echter wel tegen vrij cryptische formuleringen aan als "2009-02-01 18:50:32 DROP TCP 147.46.10.58 84.198.183.112 2089 57163". Goed om weten is alvast dat het eerste ip-adres (147.46.10.58 in dit geval) afkomstig is van de broncomputer (waar dus het verkeer vandaan kwam). Tik je dit adres in op www.samspade.org, dan kom je normaliter te weten wie dat ip-adres heeft geregistreerd (in ons voorbeeld blijkt dat de universiteit van Seoul te zijn). Het cijfer achteraan (57163) is de poort waarlangs de indringer (?) toegang zocht tot je pc. Sommige poorten blijken erg populair bij Trojaanse paarden en andere ongein. Zoek in Google maar eens naar *port trojan*: je krijgt dan meteen een reeks sites opgelijst die verdachte poortnummers hebben verzameld en becommentarieerd. Zo blijkt poort 57163 wel vaker gebruikt te worden door Trojaan BlackRat...



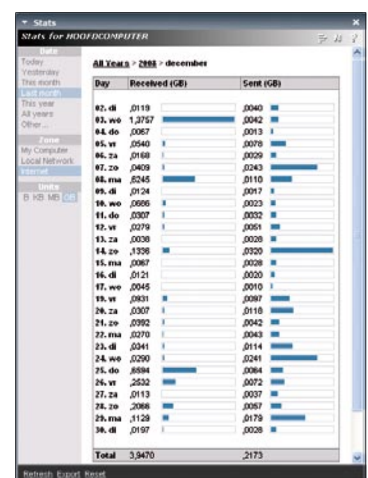
Standaard houdt Windows Firewall geen logboeken bij.

Andere firewalls

Ook andere firewalls houden informatie bij in hun logboeken. Neem nu het populaire ZoneAlarm Free www.zonelabs.com. Als je hier het hoofdvenster opent en **Alert & Logs**, **Log Viewer** selecteert, krijg je net zo goed ip-adressen en aanverwante technische termen naar je hoofd geslingerd. Het grote verschil met Windows Firewall is dat ZoneAlarm elk item een veiligheidsindicatie (rating) meegeeft, zodat je beter weet waar je moet op focussen.

Internetverkeer 

De led'jes op je router flikkeren soms wild om zich heen, terwijl je niks aan het downloaden bent? Of je provider stuurt je een mail met de melding dat je downloadlimieten alweer zijn overschreden? Installeer dan de gratis tool NetLimiter 2 Monitor www.netlimiter.com – tenzij je opteert voor de commerciële variant, die het onder meer ook mogelijk maakt dat je per toepassing een bandbreedtelimiet instelt. Na de installatie nestelt de tool zich in je taakbalk. Met een dubbelklik roep je het hoofdvenster op en zie je voor elke applicatie afzonderlijk het gegenereerde netwerkverkeer, zowel inkomend als uitgaand. Het programma houdt echter ook nauwgezet een logboek bij van al dit netwerkverkeer. Open hiervoor het menu **View** en kies **All tools**, **Stats.** Je krijgt dan een gedetailleerd overzicht van het aantal ontvangen en verstuurde gegevens over een instelbare periode, zowel binnen je eigen netwerkje als tussen je pc en het internet.



Waar gaan al die bitjes heen?

Antimalware

Van een firewall naar antimalwaretools is maar een kleine stap. Beginnen we met antivirusprogramma's. Standaard voorziet Windows niet in zo'n tool, maar er bestaan genoeg commerciële en zelfs gratis alternatieven. Tot deze laatste categorie horen onder meer PC Tools AntiVirus www.pctools.com, AVG Anti-Virus www.grisoft.com, Avira AntiVir Personal www.avira.com en avast! Home Edition www.avast.com. De meeste van deze tools houden op zijn minst een lijst bij met de bedreigingen die werden gedetecteerd, evenals de handeling die het programma vervolgens heeft uitgevoerd – al dan niet na jouw tussenkomst. Zo kan de toepassing het virus verwijderen, het verdachte bestand compleet vernietigen of het in quarantaine plaatsen.

Bij deze laatste optie kan het best interessant zijn om er regelmatig het quarantaine-logboek op na te slaan en de items op een later tijdstip nogmaals aan een scanronde te onderwerpen. Het is namelijk niet uitgesloten dat de antivirustool dankzij een update intussen wel over de nodige kennis beschikt om de gewraakte bestanden van hun infectie te ontdoen, zodat ze weer bruikbaar worden.

Naast specifieke antivirustools zijn er ook tools die zich meer richten op andere vormen van malware, waaronder Trojaanse paarden en venijnige spyware. Zo tref je in Vista de tool Windows Defender aan – XP-gebruikers kunnen die altijd nog gratis downloaden via www.tinyurl.com/defenderspyware. Ook dit programma houdt een geschiedenis bij, die zich laat openen via de gelijknamige optie in het hoofdvenster. Net als bij antivirusprogramma's tref je hier ook een link aan naar **Items in quarantaine**. Heb je bijvoorbeeld per ongeluk een programma in quarantaine gestopt, dan kan je die actie hier alsnog ongedaan maken of het item definitief vernietigen.

HIJACKTHIS

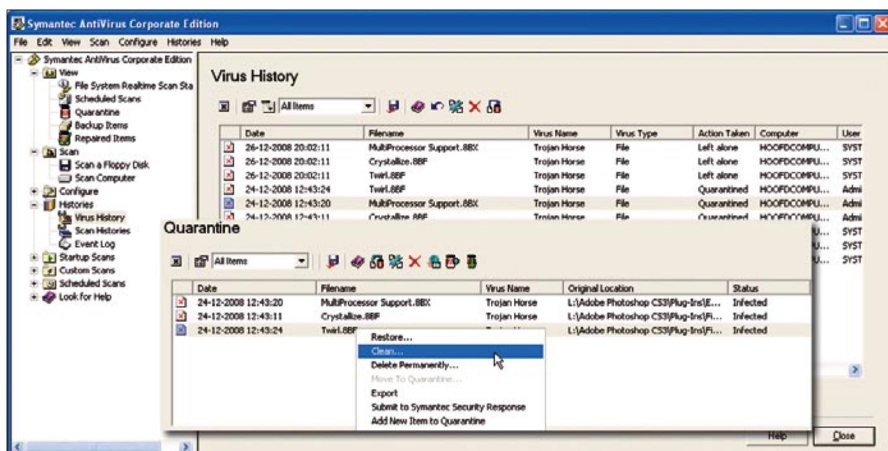
Soms weet een stukje malware toch in je systeem door te dringen: je merkt bijvoorbeeld dat er ongevraagd allerlei vensters in je browser en/of op je bureaublad opduiken. Krijg je het onding maar niet weg, dan kan je nog de hulp van een gespecialiseerde tool inroepen, zoals het gratis HijackThis www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis. Na installatie druk je op de knop **Do a system scan and save a logfile**. Het resultaat is een logbestand met wellicht vele tientallen items, waarvan de meeste door een code voorafgegaan worden (zoals R0 of F2). De precieze betekenis van deze codes kom je te weten via de knop **Info**. Je kan echter ook per geselecteerd item meer gedetailleerde informatie opvragen met de knop **Info on selected item**. Als je hierover inderdaad feedback krijgt, lees je normaliter ook af wat de tool standaard met dit item doet wanneer je de knop **Fix checked** zou indrukken. Let wel: heel vaak wordt het gewoon uit je systeem verwijderd! Wees dus zeker van je zaak vooraleer je deze knop indrukt. Veiligheidshalve doe je er wellicht beter aan het complete logboek in het online document van www.hijackthis.de te plakken of het logbestand naar deze stek te uploaden. Deze gratis service analyseert het bestand dan meteen en geeft je per item eventueel ook een indicatie, gebaseerd op het oordeel van andere gebruikers. Of je plakt de inhoud van het logbestand in een gespecialiseerd gebruikersforum, bijvoorbeeld op www.hijackthis.nl/forum. Het is lang niet uitgesloten dat je hier de nodige informatie vergaart om de onverlaat toch weer uit je systeem te kunnen kieperen. ♦

Actions	Entry	Kind	Visitor's assessment	Information
	Logfile of Trend Micro HijackThis v2.0.2			This should be the newest version.
	Platform: Windows XP SP3 (WinNT 5.01.2600)			
	MSIE: Internet Explorer v7.00 (7.00.6000.16762)			This should be the newest version.
	Boot mode: Normal		Safe	This entry was classified from our visitors as good.
	C:\WINDOWS\System32\smss.exe		Very safe	This entry was classified from our visitors as good.
	C:\WINDOWS\system32\winlogon.exe		Very safe	This entry was classified from our visitors as good.
	C:\WINDOWS\system32\services.exe		Safe	This entry was classified from our visitors as good.
	C:\WINDOWS\system32\lsass.exe		Very safe	This entry was classified from our visitors as good.
	C:\WINDOWS\system32\svchost.exe		Safe	This entry was classified from our visitors as good.
	C:\Program Files\Windows Defender\MsMpEng.exe		Very safe	This entry was classified from our visitors as good.
	C:\WINDOWS\System32\svchost.exe		Very safe	This entry was classified from our visitors as good.
	C:\WINDOWS\system32\ZoneLabs\vsmon.exe		Very safe	This entry was classified from our visitors as good.
	C:\Program Files\DigitalPersona\Bin\DPWinLct.exe			

Het resultaat van een geautomatiseerde, online analyse met HijackThis.

VAKTAAL

COOKIE: Als je bepaalde websites bezoekt, krijg je soms ongemerkt een cookie op je harde schijf. Dat is een onschuldig klein tekstbestandje dat informatie bevat over je bezoek, zoals taalvoorkeur, gebruikersnaam, datum van je laatste bezoek, enzovoort. Op die manier 'onthoudt' de website je vorige bezoekje en moet je niet bij elk bezoek alle gegevens opnieuw ingeven.



Check regelmatig de inhoud van de quarantaine (hier: Symantec AntiVirus).

